Time-Resolved Encrypted Data Comparison With Non-Encrypted Processor-Associated Signals as Detected by Bluetooth Chipsets Jeopardizes Public-Key Encapsulation-Based Security

13 August 2025

Simon Edwards
Research Acceleration Initiative

Introduction

A novel potential cybersecurity threat involves an innovative use of WiFi and/or Bluetooth chips frequently integrated into computer systems in order to exfiltrate data. Although the concept of extrapolating un-encrypted data content by eavesdropping for processor-associated signal leakage is not new, this attack would use intercepted signals to capture data concerning signals associated with the decryption process, itself in order to determine precisely what functions are being performed in order to transform data from its encrypted state to its plaintext state.

Abstract

If an intruder who has gained access to a system were to capture and attempt to exfiltrate plaintext information, even if the plaintext information were uniquely encrypted prior to exfiltration, this would almost certainly be heuristically detected. Heuristic analysis has become advanced to the point where must of cybersecurity now revolves around entirely evading it. Efficiently accessing public-key encrypted data is far from impossible, but is technically complex and time-consuming.

Rather than attempting to exfiltrate plaintext data via a network connection, radio-frequency monitoring of signal leakage from a processor (most likely through the WiFi and/or Bluetooth integrated chipsets,) this attack would serve to extract not data, but information concerning processor activity associated with the decryption process, itself. That information could subsequently be used in order to deduce key information as well as overarching principles concerning the public-key scheme which are consistent regardless of the key used.

Provided a capability to intercept the encrypted data and provided a means of exfiltrating the raw processor signal leakage information (this could be accomplished by using the Bluetooth chipset both capture and to transmit the data to a cellular device carried by the operator, for example, by bypassing the Central Processing Unit.)

Most heuristic analysis regimes watch for things such as increased processor utilization, disk read and disk write activity. Because the encrypted data would be intercepted and exfiltrated from a separate point of intercept and because the decryption-associated signal leakage raw data would never pass through the Central Processing Unit, data could be exfiltrated while bypassing heuristic detection. This is possible because the Bluetooth chipset has its own co-processor which is capable of operating entirely independently. If re-programmed, it can listen for signals and store small amounts of data in a

buffer in order to re-transmit intercepted signals at increased amplitude so that a nearby cellular device which has been compromised may be used to convey the raw data.

When the raw data reaches the adversary, it may be scrutinized for useful information and compared against the encrypted packets, using the time of arrival in order to make informed assumptions concerning which decryption steps are associated with which encrypted packets.

Conclusion

It has been repeatedly discovered that chipsets such as the Bluetooth chipset may be remotely activated despite being purposefully turned off and that most organizations utilize off-the-shelf laptops which come equipped with these chipsets. It has also been historically demonstrated that cellular devices, which are even less secure than the laptop end-points within supposedly secure networks, are carried on the person of nearly all operators at all times.

The consequence and primarily usefulness of this type of attack would be to gather large quantities of information concerning the inner workings of public-key encryption schemes such as RSA so that intercepted encrypted data may be efficiently decrypted without the need to launch attacks into specific networks.